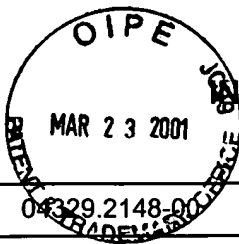


**INFORMATION DISCLOSURE CITATION**  
(Use several sheets if necessary)

Atty. Docket No. 04329.2148				Serial No. 09/377,064			
Applicants Shinichi KAWAMURA et al.							
Filing Date August 19, 1999				Group			
<b>U.S. PATENT DOCUMENTS</b>							
Examiner Initial*		Document Number	Date	Name	Class	Sub Class	Filing Date If Appropriate
<i>WJA</i>		3,962,539	06/08/76	EHR SAM, et al.			
<b>FOREIGN PATENT DOCUMENTS</b>							
		Document Number	Date	Country	Class	Sub Class	Translation Yes or No
<b>OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)</b>							
<i>WJA</i>	KOCHER, P.C., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", Springer-Verlag, pp. 104-113, (1998).						
<i>WJA</i>	ANDERSON, R. et al., "Tamper Resistance - a Cautionary Note", The Second USENIX Workshop on Electronic Commerce Proceedings, pp. 1-11 (1996).						
<i>WJA</i>	KOCHER, P. et al., "Introduction to Differential Power Analysis and Related Attacks", Cryptography Research, Inc., pp. 1-7 (1998).						
Examiner	<i>Matthew B. Smith</i>			Date Considered 6/18/03			
*Examiner:	Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.						
Form PTO 1449				Patent and Trademark Office - U.S. Department of Commerce			



OMB No. 0651-0011

**INFORMATION DISCLOSURE CITATION**  
(Use several sheets if necessary)**RECEIVED**  
MAR 26 2001  
Technology Center 2100

Atty. Docket No.	04329.2148-00	Serial No.	09/377,064
Applicant	Shinichi KAWAMURA et al.		
Filing Date	August 19, 1999	Group:	2766

**U.S. PATENT DOCUMENTS**

Examiner Initial*	Document Number	Date	Name	Class	Sub Class	Filing Date If Appropriate

**FOREIGN PATENT DOCUMENTS**

	Document Number	Date	Country	Class	Sub Class	Translation Yes or No
<i>MPA</i>	WO 9948239	09/23/99	WIPO			English Abstract

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

<i>MPA</i>	D. Coppersmith <i>et al.</i> , A Proposed Mode for Triple-DES Encryption, IBM J. RES Develop, Vol 40, No. 2, March 1996, pg 253.
<i>MPA</i>	P. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, XP 000626590, August 18, 1996, Stanford, CA

Examiner	<i>Matthew D. Smith</i>	Date Considered	<i>6/18/03</i>
----------	-------------------------	-----------------	----------------

\*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.